Guidelines on using passwords

Center for Information Technology, Kansai University

1 Purpose of these guidelines

The purpose of these guidelines is to specify what should be understood in advance, so that account users can properly manage their passwords. Additionally, we should select how to set up a proper password based on the specifications of the information system that we are using. As optimal security measures also change with threat trends, it is desirable that users regularly obtain information to review the measures.

2 Intended audience for these guidelines

(1) Audience

The intended audience for these guidelines includes all members who use accounts for the university's information system for educational or research purposes (hereinafter referred to as "users").

3 Setting and managing passwords

(1) Changing the default password

Users shall immediately change the default password to a more secure one. Do not use a password that is used for any other information services or was used in the past for the university information system.

(2) Strings used for passwords

A password string set by a user shall meet the requirements set forth in following items 1 to 3:

1) The string must be 8-16 characters long.
2) The string must include two or more lowercase alphabet letters.
3) The string must include one or more numbers.

Using passwords used in the past or passwords very similar to such passwords could lead to significantly lowered security. This is not recommended.

Do not use strings to which any of the following items 1 to 4 apply for passwords, either:

1) A string that third parties can easily guess based on user accounts. This applies to a user's name or user ID.
2) A string created by changing the order of letters of the above or adding numbers and/or symbols to the above.
3) A headword of a dictionary.
4) A proper noun such as a famous person's name.

Including uppercase alphabet letters and special symbols in a password is likely to enhance security. Symbols that can be included in user passwords for the university information system are as follows:

! # $ & ( ) * + - . ; : < = > ? @ ~ [ ] ^ _ { | } /

(3) Changing passwords

If Center for Information Technology detects information security related risks, the center can instruct users to change their passwords. Users will change their passwords without delay if they are instructed to so do by the center. Additionally, if users themselves detect disclosure or unauthorized use of their passwords, it is desirable that they immediately change their passwords.

It is not a prerequisite as an information security measure to change passwords regularly. It has been recommended to "change passwords regularly" and "use diverse strings with symbols included" as an appropriate way of managing passwords. Such measures are not sufficient, however, from the point of combating brute-force attacks. If passwords are changed regularly, it can make them easier to guess, posing a security risk. For this reason, in line with the current trend, it is recommended to "use long strings" rather than to "change passwords regularly." A long string refers to a string that contains at least 9 letters. A password created by combing initials of meaningful strings is often called a passphrase. It is desirable to create a stronger password by combining "a long string" and "a diverse string with symbols included."

(4) Managing passwords

It is desirable to observe the following 1 to 3, in order to manage passwords appropriately:

1) Do not tell your password to others.
2) Take the utmost care not to let others know your password.

3) Try not to forget your password.

It is desirable to use one of the following means 1 to 3 when storing your password in written form or on electronic media:

1) Redact a part of the string comprising the password.
2) Store the password in a place in which it can be protected securely using a physical means such as a key.
3) Use a password management application and protect access to it in some way.

4 Password-related procedures

(1) Procedures in case of password loss

If a user loses or forgets a password, such user is able to reset it through prearranged procedures. To reset the password, at the Center for Information Technology service counter, respective offices of Takatsuki Campus / Takatsuki Muse Campus, or Sakai Campus PC Class service counter, show the relevant ID (student ID or staff ID) and apply for a password reset.

(2) Reporting a password incident

If a user detects unauthorized use of an account or a risk of password disclosure, such user shall report it to the Center for Information Technology immediately.

5 Precautions for handling passwords

(1) Prohibited use of a password in a place where password fraud is likely to occur

Do not access the university information system from an off-campus Internet cafe or using public Wi-Fi. Access to the university information system using terminals or wireless services that an unspecified number of people use poses the risk that passwords or accounts could be stolen.

(2) Recommended use of a screen lock

To be away from a PC while still being logged in to it, lock the screen, so no third parties view or work with it. If you use a password to lock the screen, avoid a string that others can easily guess. It is desirable to use a password consisting of a long string.

Supplementary provisions

1. These guidelines become effective on November 6, 2019.